September 2017

Security Awareness News

the security awareness newsletter for security aware people

Being Smart About Smart Devices

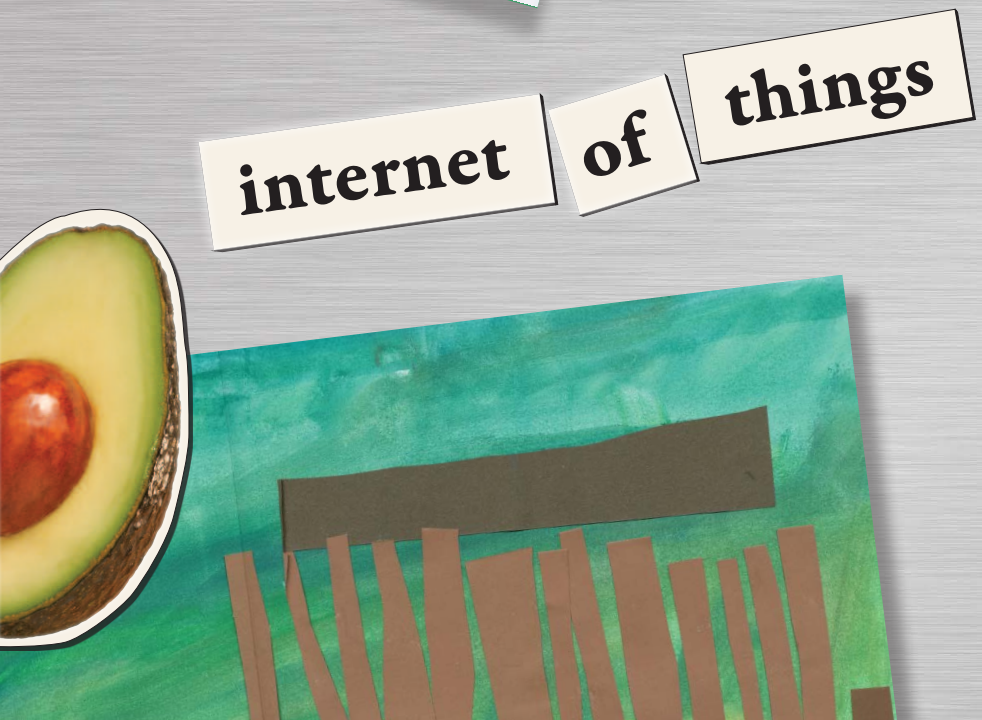
The Internet of Things
and the Concerns of Convenience

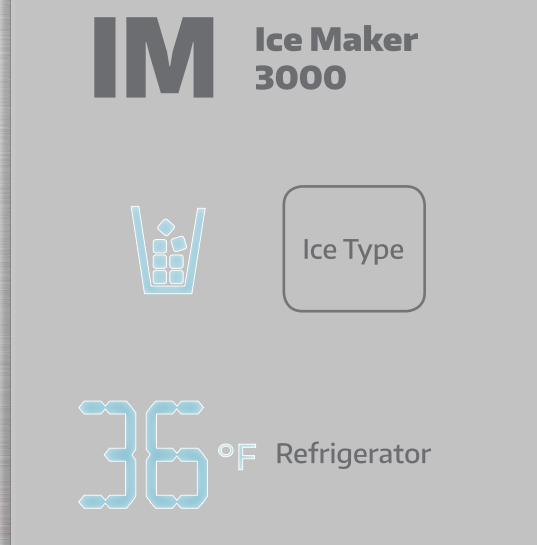
IoT Gone Rogue

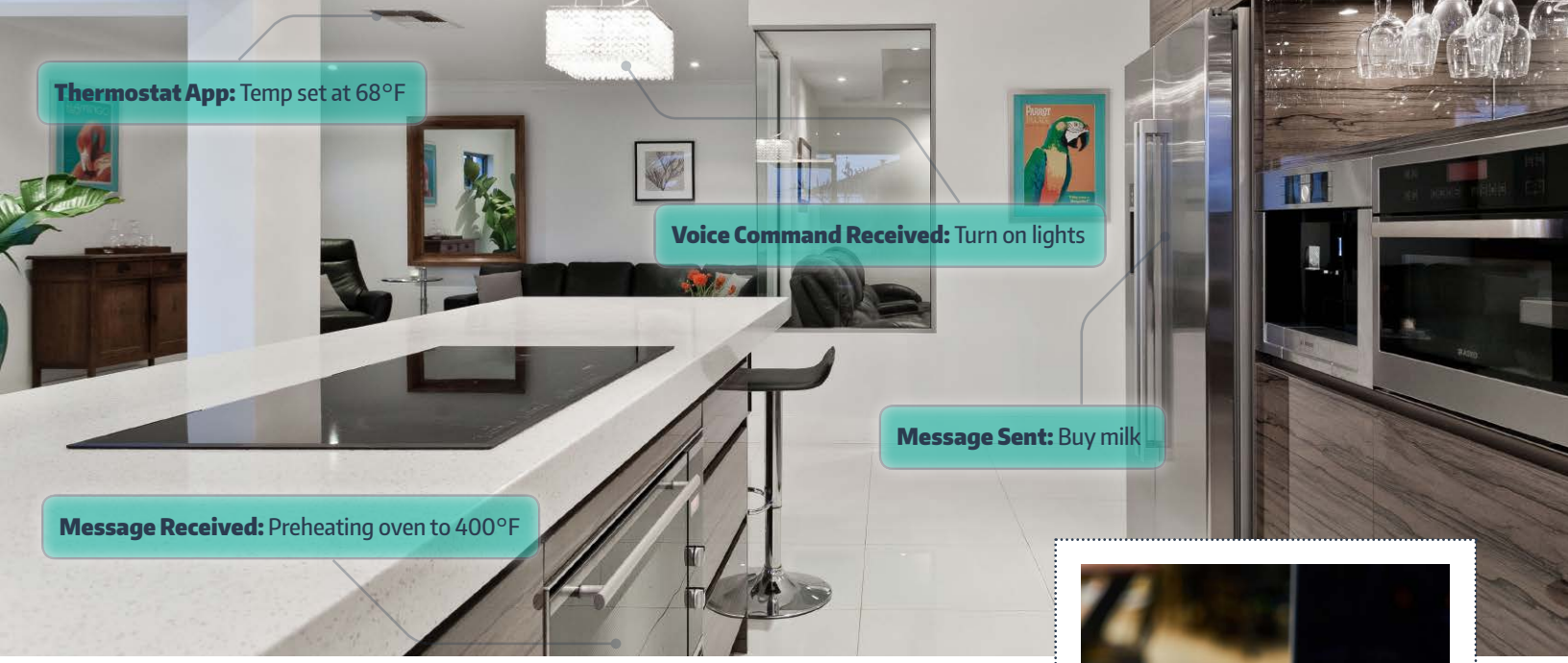
Securing Smart Devices

Where's the Remote?

PLUS BONUS INFOGRAPHIC:
How VPNs Work







The Internet of Things *and the Concerns of Convenience*

There's an old joke that goes something like:

> *"Is your refrigerator running?"*
> *"Yes..."*
> *"Well, you'd better go catch it!"*

This is what is generally referred to as a *"dad joke"* since most youngsters roll their eyes when they hear it, but it doesn't get the same laughs it used to. Thanks to the Internet of Things (or IoT), if you ask someone if their fridge is running they might pull out their smart device and tell you the exact temperature of their fridge as well as how much electricity they're currently saving. They may even show you the notification from their fridge telling them to buy milk.

That's our world now. Your washing machine updates your online shopping list with detergent. You can tell your digital assistant to play classic rock and dim the lights. You can change the temperature in your home from your mobile device while traveling internationally.

And it's more than just the convenience of cool gadgets. The healthcare industry has embraced IoT, with one report claiming the global healthcare sector will invest upwards of $400/€340 billion by 2022. The IoT will improve health services with technology that monitors patients, sends alerts to physicians, and monitors machines to ensure they don't lose power. By harnessing the IoT, hospitals can effectively reduce response time and improve patient care.

In its current state, the IoT is a huge security risk.

But there is a dark side to the IoT. Maybe you've already experienced it. If you lived on the East Coast of the United States in October of 2016, you probably lost access to major websites when a botnet, powered by compromised IoT devices, attacked a major server. In its current state, the IoT is a huge security risk. Between end-users failing to check security settings and tech companies rolling out new products without proper security safeguards, the network of smart devices is alarmingly vulnerable. In the realm of healthcare, for example, the IoT's vulnerabilities could have perilous effects on people's lives.

WHAT CAN YOU DO ABOUT IT?

Learn about any security controls in every IoT device you use.

Immediately update new devices with unique logins and passwords. The default settings and passwords for most devices are public knowledge, thus making security risks even greater.

Keep those devices up to date. Patches are released to fix security holes.

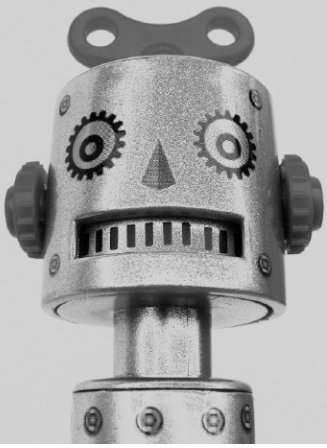
Consider whether every device you own truly needs an internet connection.

Here at work, always follow policy and be sure to ask before connecting any device to our network!

Good security comes from timely response. Report security incidents immediately!

IoT GONE ROGUE

An Army of Idiots



Here's the thing about smart devices: **they're not that smart.** Sure, they communicate with each other and perform cool tasks that were once only science fiction, but that's where their intelligence ends. IoT devices aren't smart because they can be easily manipulated.

The lack of built-in (native) IoT security means cybercriminals can infect these devices with malware and make them part of a global botnet. Botnets are armies of compromised devices, from your home router to bank security cameras. Under the control of malicious persons, botnets aim to inhibit or damage internet services. Some botnets overwhelm servers with vast amounts of traffic, causing them to crash (known as a **DDoS attack**).

Why would anyone do this? It could be bored pranksters having fun. It could also be a nation-state attacking critical infrastructure (cyberwarfare), a group shutting down a website to push an agenda (hacktivism), or even a company attempting to gain a competitive advantage by shutting down their competitor's website or payment systems. Results may vary but they're seldom positive.

DEFINITION: DDoS
(distributed denial-of-service)

A cyber-attack in which the victim's server is overwhelmed with traffic from perhaps thousands of sources, effectively rendering it unusable.

Remember Mirai?

In October of 2016 criminal hackers used a malware strain known as Mirai to compromise an estimated 100,000 devices in the largest DDoS attack to date. The attack knocked major websites offline for hours at a time in both Europe and North America. Although it may seem minor that services such as Netflix and Spotify were unavailable for consumers, this attack illustrates how dangerous the IoT can be when we don't implement proper safeguards!

How Many Devices Are There?

A couple of years ago, Cisco released a white paper predicting that, by the year 2020, the world would play host to some *50 billion* connected devices, including everything from smart TVs to automobiles. How close are we to realizing that prediction? According to statista.com, there were *17.6 billion* connected devices in 2016 with another three billion expected in 2017. The IoT is a growing trend still very much in its infancy. As more and more industries embrace the capabilities of IoT, the number of connected devices is expected to surpass *75 billion over the next eight years!*

That is a massive number of devices, and a massive attack surface for cybercriminals worldwide. Hopefully manufacturers will make more of an effort in the near future to improve security. Until then, it's on us—the end-users—to take additional steps in securing our devices.

Good security comes from timely response. Report security incidents immediately!

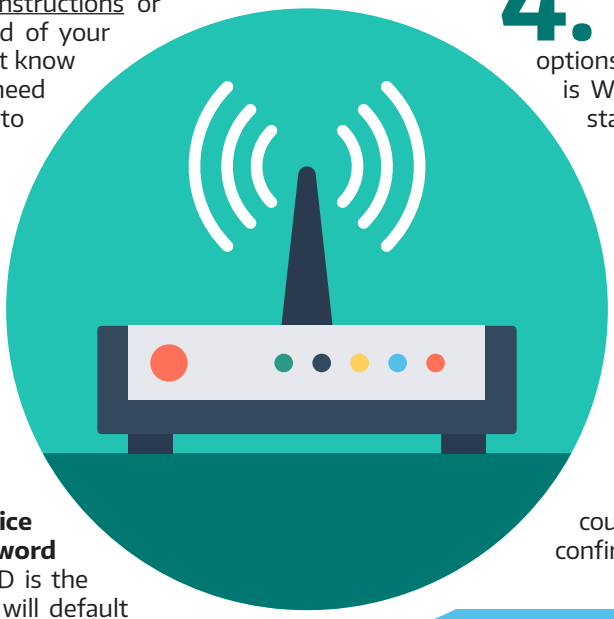
Securing Smart Devices

6 Steps to Configuring Your Home Router... Properly.

1. **Log in.** Use your router's IP address, which can be found by following these instructions or simply looking up the brand of your router in a search engine. (If you don't know the username or password, you will need to hard-reset the router, returning it to factory settings.)

2. **Change the default admin username and password ASAP.** Most new routers, or recently reset routers, have the username and password default set to "admin". Clearly, leaving it set to default is a major security fail. You can verify the login credentials of your router by going here.

3. **Change the SSID (Service Set Identifier) and password of your network.** The SSID is the name of your wireless network and will default to something basic determined by the manufacturer. Change it to something unique and protect it with a strong password.



4. **Choose the right encryption.** When you setup your new SSID and password you will likely see a few options for encryption. The one you want is WPA2 + AES. This is the most secure standard to date.

5. **Upgrade the firmware.** Like all connected devices, your router will have occasional firmware upgrades. These upgrades often patch security holes. It's a good idea to routinely log in and check for new updates.

6. **Periodically check the security settings.** Things can happen. It only takes a couple of minutes each month to check, confirm, and, if necessary, update.

Should you hide your SSID?

Most routers allow you to hide your SSID, which means no one else can see—or connect to—your network. But it's not actually a security feature. Not only could it cause connection problems, but there are plenty of free utilities out there that will discover hidden networks with a single click. **In fact, hiding your SSID could be more of a security risk than a safeguard.** Read why here: https://www.howtogeek.com/howto/28653/debunking-myths-is-hiding-your-wireless-ssid-really-more-secure/ .

Defending Your Devices

Worried that your Amazon Echo or your DVR could be compromised? Follow these seven steps to defend your devices against cyber threats!

ONE • Research devices before purchasing. Read reviews by security experts. If they don't have customizable security controls, seriously reconsider.

TWO • Change usernames and passwords right out of the box. Defaults are a major security risk.

THREE • Turn on auto-update wherever possible. This will ensure you don't miss important security patches.

FOUR • Keep an ongoing list of the devices on your network. Most routers do this for you. Print out a map of your home network.

FIVE • Disable any devices that don't need an internet connection as well as features you don't use.

SIX • If possible, consider a wired connection instead of wireless.

SEVEN • Disable Universal Plug and Play features. Convenience isn't free.

BYOD?

BYOD is short for *"bring your own device,"* which refers to employees bringing their own phones, tablets, and computers to their place of work. As you can imagine, BYOD presents numerous challenges for organizations to overcome. On one hand, allowing employees to access company networks and intranets with personal devices may improve productivity and encourage remote work, especially in a travel-oriented society. On the other hand, *BYOD adds risk because – in a mobile world – there is serious potential for data and devices to be lost, stolen, or otherwise compromised.*

What does it mean for you here at work? It's quite simple: *always follow policy.* Know which devices you can bring to work, if any, and which parts of our network those devices are allowed to access. If you're not sure what our BYOD policy is and whether remote access may be allowed, *don't hesitate to ask!*

Good security comes from timely response. Report security incidents immediately!

WHERE'S THE REMOTE?

The ability to work away from the office comes with added responsibilities, and this goes for computer security basics as well. Remote workers still need to follow standard security protocols, such as using strong passwords, updating devices, and remaining suspicious of random links and attachments. But the basics aren't enough! Think about it like this; where you go, your devices go. And where your devices go, your information goes.

THE TOP THREE THREATS WE FACE WHEN WORKING REMOTELY:

SHOULDER SURFERS. When remotely accessing sensitive information of any kind, be sure no one is looking over your shoulder or spying on your screen. Never forget the "Human Domain!"

THIEVES. The physical domain means we need to watch out for more than cybercriminals. We also need to stay alert for real-life thieves. Never let your devices out of your control - ever!

PUBLIC WIFI. Perhaps the biggest threat, public Wi-Fi invites a host of Cyber Domain security issues. Avoid accessing or sending ANY sensitive information when connected to public networks unless you know how to do so securely and within our policy guidelines.

5 NON-TECHNICAL WAYS TO STAY SAFE WHILE WORKING REMOTELY:

USE A VPN WHEN CONNECTING TO A PUBLIC NETWORK. VPNs, short for virtual private networks, encrypt your connection and make it nearly impossible for a criminal to hijack your information. This may sound technical, but VPNs today are a "One Click" or automatic app. Be sure to follow policy on VPNs!

BE DISCREET. If you're in a public setting and conducting private business, make sure no one can overhear your discussions or spy on your screen.

GET A PRIVACY SCREEN COVER. A privacy screen cover adds yet another layer of security. You must have a direct, centered view in order to see what's displayed on laptops, phones, and tablets.

KEEP TRACK OF INVENTORY. When traveling, keep all devices (and anything with sensitive info) on your person or in your sight at all times. Never trust strangers to "watch your stuff."

AVOID USING REMOVABLE STORAGE. USB flash drives and other external data storage devices are easy to lose and easy to steal. If you must use them, encrypt and password protect them.

WHAT SHOULD *you* DO IF A DEVICE IS LOST OR STOLEN?

FOR PERSONAL DEVICES

Most manufacturers enable remote features that allow you to locate, lock, or erase your device. If you believe your smartphone, for example, is lost, you can log in to your account via a web browser and ping it to ring. You can also lock it with a new password. In a worst-case scenario, you can remotely reset your device back to factory default, which erases all information. Experts recommend that you enable these features and know how to access them for all devices. Find out more about MDM, Mobile Device Management, here: https://en.wikipedia.org/wiki/Mobile_device_management.

FOR WORK-ISSUED DEVICES

If a work-issued device has been lost or stolen, report it immediately. The quicker you let us know, the quicker we can take the appropriate steps towards protecting sensitive information!

Good security comes from timely response. Report security incidents immediately!

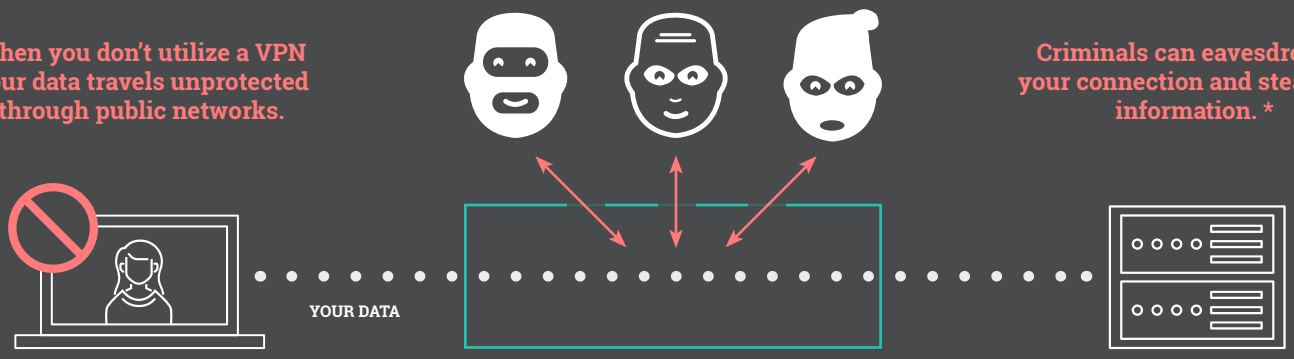
How Do VPNs Work?

VPN stands for Virtual Private Network. It adds an extra layer of security when you are surfing the web on public or private networks.

WITHOUT A VPN

When you don't utilize a VPN your data travels unprotected through public networks.

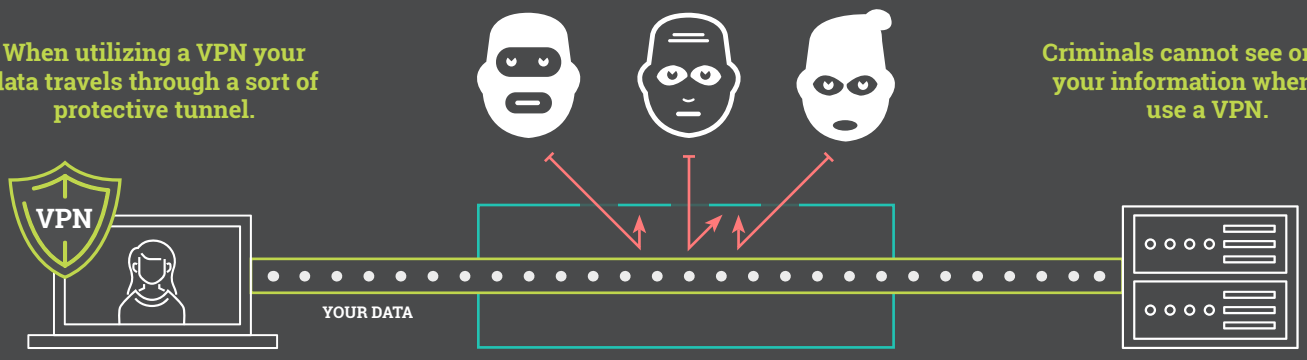
Criminals can eavesdrop on your connection and steal your information. *



WITH A VPN

When utilizing a VPN your data travels through a sort of protective tunnel.

Criminals cannot see or steal your information when you use a VPN.



It's *always* a good idea to use a VPN!

* There is no such thing as perfect security, so even on a VPN, you should still be cautious when logging into personal accounts when on public networks.

Good security comes from timely response. Report security incidents immediately!